REMARKS

Reconsideration of the application is respectfully requested for the following reasons:

1. Formalities

Figs. 6-9 have been labeled as –prior art–, and the various missing reference numerals have been added to Figs. 1-3, as required in items 4 and 5 of the Official Action.

The first four lines of page 8 have been deleted to eliminate the redundancy noted in item 3 on page 2 of the Official Action.

2. Rejection of Claims 1-24 Under 35 USC §112, 2nd Paragraph

This rejection has been addressed as follows:

a. Each of independent claims 1, 7, 13, and 19 has been amended to define p(x) as a primitive polynomial that can construct a finite field, in which an element of α that is a root of p(x) can be defined so that $p(\alpha) = 0$, the finite field consisting of $\{0,1,\alpha, \ldots, \alpha^{2^{(m-2)}}\}$. This definition of p(x) is well-known to those skilled in the art and therefore does not represent "new matter." It also follows from the fact that the polynomial p(x) is by definition irreducible ("non-reducible"), as explained in lines 6-7 on page 8 of the original specification, and from equations 1-7 on page 8 (particularly equations 4 and 7).

b. Each of the independent claims has also been amended to clarify that matrix A is not "expanded" into matrix form, but rather is –decomposed–. The elements of matrix A and vectors B and C make up the finite field. Each of them has m bits. In order to perform the finite-field multiplication, *i.e.*, A x B = C, the finite-field element A is decomposed into an mxm matrix of which columns are represented by elements A, $A\alpha$, ... ,$A\alpha^{m-1}$, as explained in the last four lines on page 7 of the original specification, and indicated by element 11 of Fig. 2, in which elements 113 (XORs) are applied to the decomposition (or expansion). The finite-field element B is expressed by an mx1 matrix (or vector) based

on its m bits. Hence, an mxm matrix is multiplied with an mx1 matrix to generate an mx1 matrix for the finite-field element C, with multiplication of the matrix elements and addition of their products to obtain a polynomial being carried out in the embodiment illustrated in Figs. 2 and 5 by the AND and XOR functions or elements.

c. Claim 13 (as well as the other independent claims) has been amended to define α in terms of p(x), as explained above.

d. Finally, the characterization of lines 5-6 in claim 13 as mis-descriptive is respectfully traversed on the grounds that the elements of each column are in fact sequentially generated by parallel column-based matrix vector generator, as explained in lines 4-8 on page 5 and lines 1-2 on page 6 of the original specification. This follows from the shifting procedure described in the paragraph bridging pages 10 and 11 of the specification, which inherently is a sequential procedure.

Having thus overcome the sole rejection and each of the objections made in the Official Action, and in view of the indicated allowability of claims 1-24, expedited passage of the application to issue is requested.

Respectfully submitted,

BACON & THOMAS, PLLC

By: BENJAMIN E. URCIA
Registration No. 33,805

Date: June 17, 2004

BACON & THOMAS, PLLC
625 Slaters Lane, 4th Floor
Alexandria, Virginia 22314
Telephone: (703) 683-0500